Chapter 1

Network Architecture

This section gives an overview of the most important entities in a GSM network and the different protocols that are used between these entities.

A single GSM network is often referred to as a Public Land Mobile Network (PLMN). This is the network operated by a single provider in a single region. In most countries each provider maintains a single PLMN, but in certain large countries, like the USA, several PLMNs can be maintained by a single provider. A PLMN manages all traffic between mobile phones and all traffic between mobile phones and the other land networks. These land networks can either be the Public Switched Telephone Network (PSTN), an ISDN network, or the Internet. Figure 1.1 shows an overview of all the entities in a GSM network.

These entities are often subdivided between three "domains"; the Mobile Station (MS) – i.e. mobile phones – , the Base Station Subsytem (BSS) and the Network Switching Subsystem (NSS). We will now look at each of these in more detail.

1.1 Mobile Station (MS)

The Mobile Station (MS) is the subscribers module most people are familiar with. It consists of both some Mobile Equipment (ME) and a Subscriber Identity Module (SIM). Both are needed for the Mobile Station (MS) to function in the GSM network. Hence MS = ME+SIM.

1.1.1 Mobile Equipment (ME)

The Mobile Equipment (ME) is simply the GSM phone people use to make and receive calls in a cellular network. It is basically a transmitter-receiver unit that is independent from network providers[1].

Every ME contains an International Mobile Equipment Identity (IMEI) number, consisting of 15 digits which uniquely identify this particular ME. An ME can be asked for its IMEI by typing in the string '*♯06♯' on the mobile phone.

[1]In most countries MEs can be bought from providers in some form of packaged deal. A ME can have provider specific firmware, and can be modified to only accept the providers SIM (SIM-locking). Also some providers produce their own MEs. However, their networks still accept other MEs and their MEs can, with a small modification (SIM-unlocking), function in another network.

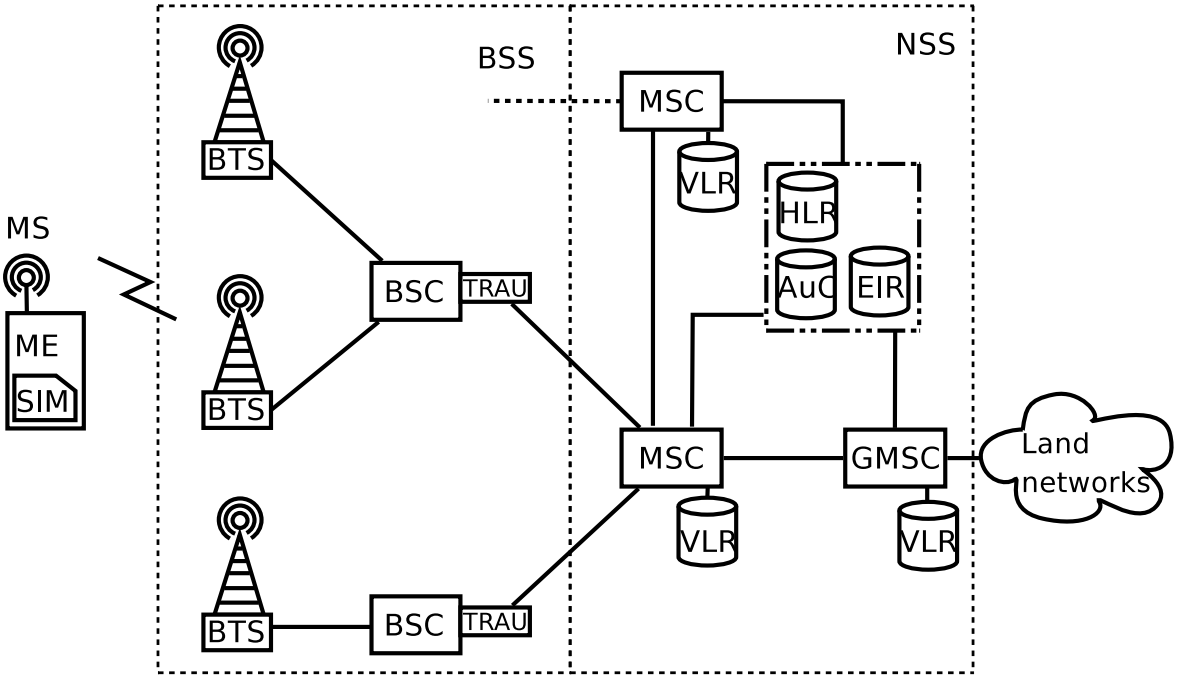

Figure 1.1: Network layout of a generic Public Land Mobile Network (PLMN).

1.1.2 Subscriber Identity Module (SIM)

The Subscriber Identity Module (SIM) is provided to a subscriber as a smart card; a SIM card. It contains a user's identity in a GSM network and is dependent on a network provider. It is uniquely identified by its International Mobile Subscriber Identity (IMSI) number. A SIM contains the following information:

- The International Mobile Subscriber Identity (IMSI).
- The Temporary Mobile Subscriber Identity (TMSI), temporary identifier passed on to the MS by the network to hide the IMSI. The TMSI is only valid within a certain region, and the MS can always request a new one from the network.
- The secret key K_i.
- The current encryption key, also called session key: K_c.
- The Ciphering Key Sequence Number (CKSN), a 3 bit number send by the network, acting as an identifier of the current session key
- Specific implementations of the encoding algorithms A3 and A8.
- The current Location Area Identity (LAI), which is transmitted by the network regularly and stored in the SIM. It identifies a certain area in the PLMN.
- List of preferred Public Land Mobile Network (PLMN)s.
- List of forbidden PLMNs.

- List of beacon frequencies of the home PLMN, these are the frequencies a MS will begin to scan when looking for cell towers.
- The Personal Identification Number (PIN) used to gain access to the SIMs functionality.
- The Pin Unblocking Code (PUK) used to reset the Personal Identification Number (PIN) and unlock the SIM, when the wrong PIN number has been entered three times.
- Storage of Short Message Service (SMS), telephone numbers, etc.

Note that the IMSI is not equal to the Mobile Subscriber ISDN Number (MSISDN), the phone number belonging to this sim. Both numbers are created independently and linked to each other in the HLR (section 1.3.3). The IMSI is the identifier in the GSM system for an MS and it belongs uniquely to a single SIM. A MSISDN is linked to the IMSI, and can be renewed.

1.2 Base Station Subsystem (BSS)

The Base Station Subsystem (BSS) is the part of the PLMN that manages the communication between the MSs and the Network Switching Subsystem (NSS).

1.2.1 Base Transceiver Station (BTS)

A Base Transceiver Station (BTS) is another name for a cell tower, or more accurately a name for the transceivers on a cell tower. One BTS defines a single cell. In general it is simply a relay station that broadcasts to the MS the packages it receives from its Base Station Controller (BSC) (next section) and vice versa. Because the Base Transceiver Station (BTS) is the link between the air interface and the land interface, it is responsible for all the channel encoding/decoding, ciphering, Slow Frequency Hopping (SFH), Gaussian Minimum Shift Keying (GMSK) and burst formatting.

'Land interface' is a somewhat misleading term to describe the link between a BTS and the rest of the network. Although most BTSs are connected via a land line, some use a microwave directional radio link for this connection. Whether through a land line or via a directional radio link, the signal uses the same Abis interface (section 1.4).

The maximum reach of a BTS is 35km. Though a transmitted signal might travel beyond this distance, the delays that occur in the transmissions become to large to still function within GSM.

A BTS can hold between one and sixteen transceivers, depending on geography and user demand in the area. Eight transceivers for the uplink frequencies (MS to BTS) and eight for the downlink frequencies (BTS to MS). Each transceiver can handle eighth different channels which MSs can use. Because some of these channels are used for sending control information, a BTS can never handle more than about 60 ($8 \times 8-$ some control channels) conversations with mobile phones in its area. However, many more phones can be connected to a cell, while not actively using it.

A BTS is identified by its Cell Global Identification (CGI). A fourteen digit number uniquely identifying this cell. It is composed of a Location Area Identity (LAI) and a Cell

Identity (CI).
There exists an open-source implementation of a BTS named OpenBTS [3]. In most countries a license is required to operate a BTS.

1.2.2 Base Station Controller (BSC)

The Base Station Controller (BSC) is the center of intelligence in the Base Station Subsystem (BSS). A single BSC controls one or more BTSs and typically serves a population of around 100,000 to 250,000 people [4]. It manages the radio channel setup and handovers from a MS between BTSs that are connected to this BSC. It also watches the status of the BSS hardware.

There exists an open-source implementation of a BSC named OpenBSC [5]. It is not specifically build to work with OpenBTS; actually both projects individually attempt to be usable as an entire BSS.

Transcode Rate and Adaption Unit (TRAU)

The BSC side of the network can also contain a Transcode Rate and Adaption Unit (TRAU). The air-interface uses a voice encoding, regular pulse excited-long term prediction (RPE-LPC), which manages a data rate of 13 kbit/s. However, the voice encoding used on the land interface, Pulse Code Modulation (PCM), reaches 64 kbit/s. The transcoding needed between these signals is performed in the Transcode Rate and Adaption Unit (TRAU). Although this transcoding is defined as a responsibility of the BSC, it is often performed by a distinct subsystem. Some vendors have implemented the TRAU at the Mobile Switching Center (MSC, see 1.3.1) side of the network, thereby compressing the signals earlier on and saving bandwidth between the BSC and the Mobile Switching Centre (MSC).

1.3 Network Switching Subsystem (NSS)

The Network Switching Subsystem (NSS) is the central part of any PLMN. A single NSS controls multiple BSSs. The NSS houses all subscriber services. It authenticates the SIM for access to the network and for setting up calls. It finds the MSs in it's region when a call is being made to it or routes the call through to the Public Switched Telephone Network (PSTN) or to a neighboring NSS for MSs outside of it's region.

1.3.1 Mobile Switching Center (MSC)

The Mobile Switching Centre (MSC) is the main component of any NSS. It is a modified version of a standard ISDN-switching system and it performs several functions:

- Manage the location (which BSC/BTS) of all MSs in its service area.
- Set up and release end-to-end connection.
- Controls handovers between BSCs.
- Manages call data and sends this to the billing system.

- Collects traffic statistics for performance monitoring

Every BSS is connected to a single MSC. All the BSSs connected to a MSC comprise its service area.

1.3.2 Gateway Mobile Switching Center (GMSC)

All communication between different PLMNs or between the PLMN and the PSTN is routed via the Gateway Mobile Switching Centre (GMSC). When a MS attempts to log-on to a different network than his home network, the GMSC of the visited network asks the GMSC of the home network to authenticate the MS. When a call request arrives at a MSC it will check whether the destined MS is within this MSCs service area. If this is not the case the request is forwarded to the Gateway Mobile Switching Centre (GMSC) which will then route the call to the correct MSC, to the PSTN, or to the responsible GMSC of another provider.

The GMSC is a special form of a MSC. The practical implementation of a GMSC can vary. Some networks contain a single, high performance MSC as dedicated GMSC, but there are also PLMNs where every MSC can function as the GMSC. In the latter case the term GMSC is only valid in the context of a single call or sign-on, because its role can be carried out by a different MSC each time.

1.3.3 Home Location Register (HLR)

The Home Location Register (HLR) contains the subscriber's information for call control and location determination. Logically there is only one Home Location Register (HLR) per provider per GSM network, although this can be implemented as a distributed database.

The HLR stores the following information per IMSI:

- The subscriber's MSISDN, i.e. the telephone number.
- The current VLR (see section 1.3.4) serving the subscriber, used to locate the MS.
- GSM services that the subscriber is allowed to access.
- Possible call divert settings.

Both the IMSI and the MSISDN fields have primary database keys over them. The HLR is where the standard phone numbers (MSISDN) are linked to their IMSIs. When a call is placed to a MSISDN, the GMSC requests the corresponding IMSI and the current MSC serving it, from the HLR. The HLR receives location updates for every IMSI in its database from the current serving VLR.

1.3.4 Visitor Location Register (VLR)

Each MSC maintains one Visitor Location Register (VLR) which stores all the SIMs that are active within the MSC's service area. When a MS is successfully logged on to an allowed PLMN, the home network's HLR is queried for some subscriber information which is stored in a record in the VLR. This happens after the VLR informs the HLR of the presence of the IMSI in its VLR area. These messages between VLR and HLR are even exchanged when the subscriber is within his own home network. The VLR can be used by the MSC to route

incoming calls to the correct BSS.

After some period of inactivity or when a MS has traveled to a different service area, the record for an IMSI is removed from the VLR. In the latter case the removal is commanded by the HLR. For every IMSI the VLR stores the following information:

- The subscribers current Temporary Mobile Subscriber Identity (TMSI), which is allocated by the VLR.
- The subscribers MSISDN.
- The subscribers current Location Area Identity (LAI), or a specific VLR is maintained for every LAI.
- The subscribers current Cell Identity (CI). The LAI and the CI together form the Cell Global Identification (CGI) and define a unique cell in every PLMN.
- GSM services that the subscriber is allowed to access.
- The HLR address of the subscriber.
- Up to five authentication triplets, received from the Authentication Centre (AuC).

1.3.5 Authentication Centre

The AuC contains the information needed to authenticate a SIM and to set up an encrypted connection with a MS (see Section 2). The AuC is often co-located with, and in most implementations even integrated in, the HLR.

In the AuC the following information is stored per IMSI:

- The secret key K_i, the same as on the SIM.
- The encoding algorithms A3 and A8, the same as on the SIM.

Despite its name, the AuC does not directly authenticate a SIM. Instead it computes a random challenge and the corresponding reply and encryption key, K_c, using the A3 and A8 algorithms. These three values form so called (authentication) triplets. These triplets are then stored at the VLR and from there supplied to the MSC where a MS tries to authenticate itself. The real authentication takes place at the MSC, which sends the random challenge to the MS (via the BSC and BTS) and verifies the MSs response. The encryption key is sent on to the BTS, because only the MS - BTS link is encrypted with it.

The implementations for the A3 and A8 algorithms are only stored and invoked on the SIM and in the AuC. Both are under control of the provider, so the specification leaves some room here for every provider to implement their own algorithms. Most providers started by following the advised implementations of A3 and A8 [6] however, it is now mostly unknown what kind of implmentation is used by which providers.

1.3.6 Equipment Identity Register (EIR)

The Equipment Identification Register (EIR) is often co-located with the HLR. It contains lists of International Mobile Equipment Identity (IMEI)s [7]. When a MS is connected to a network, the network can always give it the identify command. In response to this command the MS will transmit its IMSI, identifying the SIM, and IMEI, identifying the physical phone (ME). The IMSI ends up at the HLR, but the IMEI is checked against the stored identifiers in the EIR.

This built-in IMEI security also has several problems; it hinges on the difficulty to change a phone's IMEI, but in most mobile phone models today this proves rather simple. There also is no specified method to unblock a IMEI once it is registered in the EIR.

1.4 Interfaces

Within the GSM network several different interfaces are defined. These are all shown in Figure 1.2.

The main interfaces, those interfaces that connect a MS to the land interfaces (Um, Abis,

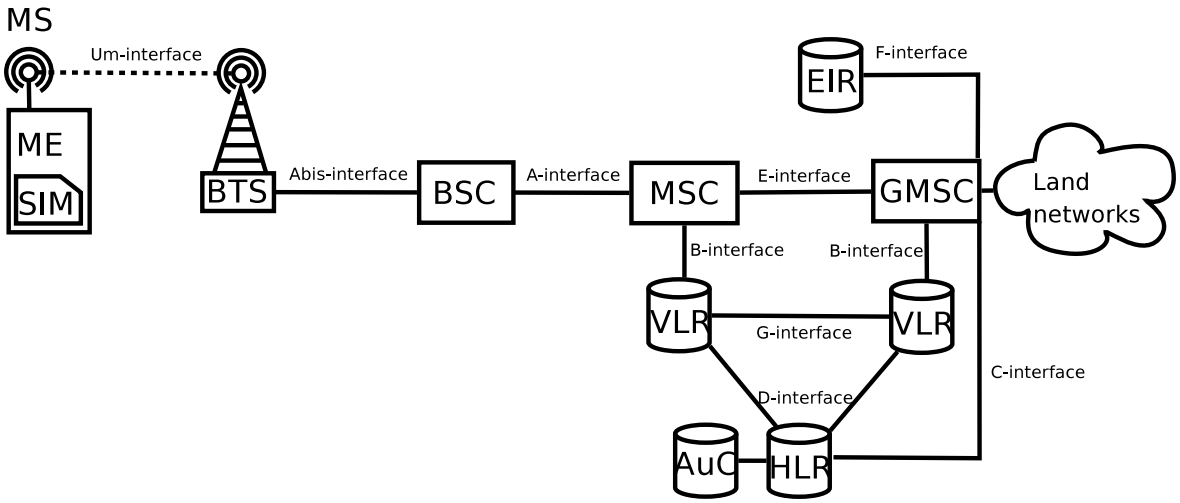

Figure 1.2: The defined interfaces within a GSM network.

A and E), are all split in traffic channels that contain the speech information and control channels on which the meta-data is transmitted.

The Abis interface connects the base stations (BTSs) to the base station controllers (BSCs). This interface is defined as an LAPD (standard ISDN) interface and largely coincides with the data link layer of the Um interface. The Abis interface also allows control of the radio equipment and radio frequency allocations in the BTS.

The A interface connects the BSS with a NSS and the E interface is the main interface inside a NSS. All the control channels on the A and E interface are part of the Signaling System #7 (SS7), a collection of telephony signaling protocols defined by the International Telecommunication Union (ITU) [8]. The TRAU (section 1.2.2) does not interfere with any

of the signaling channels. It only transcodes the voice data.

The B, C, D, F and G interfaces are defined to synchronize all the different information sources within a PLMN. The ETSI has not defined an interface between the AuC and the HLR, so every provider can make their own decision here. Most providers have the AuC located at the HLR site and often these two databases are integrated.

Chapter 2

Authentication in GSM

This chapter explains the way authentication of a MS – a mobile phone, with a subscriber's SIM card inserted – works inside a GSM network.

The most important aspect to understand is that in GSM, only the MS authenticates itself to the network, but the network never authenticates itself to the MS. This leaves GSM vulnerable for Man-In-The-Middle attacks.

The authentication of a MS to the network is of course one of the most important security functions in GSM. After a successful authentication the MS has proven its identity (IMSI) to the network and at that point both the MS and the BTS will know a shared session key, K_c, which they could use for encrypted communication.

2.1 The authentication

Both the GSM network and the MS know a common secret: a specific secrect key K_i, respectively stored at the AuC and in the SIM. The MS authenticates itself by proving to the network that it knows K_i. In order to prove this without having to transmit K_i itself, which could be intercepted, a so-called challenge-response method is used. In this method the network sends a challenge (a random number) to the MS, the MS then computes a response with a function, called A3, that uses both the challenge and the secrect key K_i as input. The network can verify if the response was indeed computed using the correct K_i, if so then the MS has proven to have access to the correct K_i and thus authenticated its identity.

Another algorithm is also used during the authentication; the A8 algorithm. This algorithm also has two input variables; the challenge and the secret key K_i, the same as in the A3 algorithm. However, this algorithm computes a session key, K_c, which *can* be used to encrypt the communication following the authentication (encryption on the communication is optional, and its use is decided by the network). This algorithm results in both the network and the MS ending up with the same session key, allowing both sides to communicate encrypted (see Chapter 3) using a key only they should be able to derive.

A somewhat simplified depiction of the authentication is shown in Figure 2.1; the variables used are explained below.

A summary of all the variables used in an authentication:

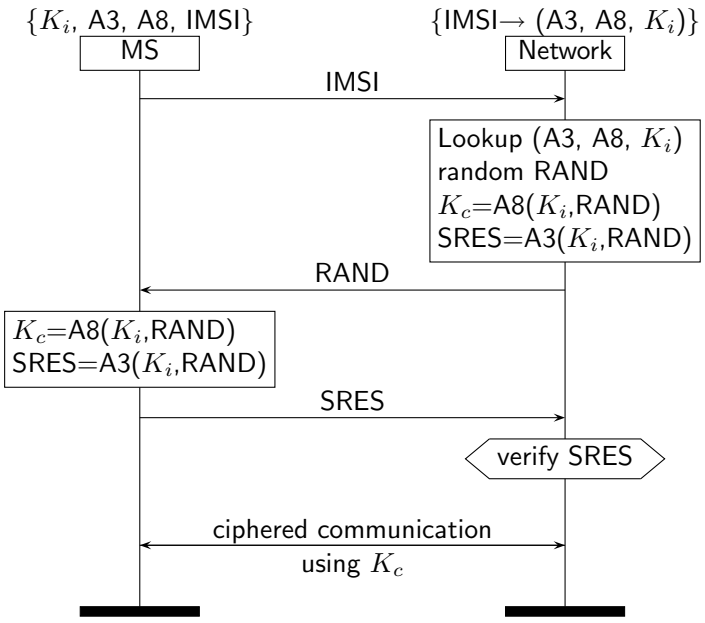

Figure 2.1: Simplified authentication of a MS to the network.

- IMSI, the unique identifier for a single SIM.
- RAND, a 128 bit random number, generated by the AuC.
- K_i, the 128 bit secret key, chosen by the provider and stored in the SIM card and at the AuC, where it is linked to a unique IMSI.
- A3, algorithm stored in the SIM card and at the AuC, see Section 2.3.
- A8, algorithm stored in the SIM card and at the AuC, see Section 2.3.
- SRES, 32 bit signed response, computed by A3(K_i,RAND).
- K_c, 64 bit session key, computed by A8(K_i,RAND).

2.2 Logistics inside the network

Within the GSM network only the SIM card of a subscriber and its provider's AuC know the secret key K_i and the specific A3 and A8 algorithms (see Sections **??**, 1.3.5 and 2.3). However, the check whether the MS's response is correct is performed by the serving MSC.

The communication inside a GSM network needed for authentication is shown in Figure 2.2. The authentication is always initiated by the serving MSC. At some point (e.g. during log-on) the MSC decides to authenticate a MS identified by an IMSI or TMSI. The MSC requests an authentication triplet (K_c,RAND,SRES) for the IMSI from the VLR. Authentication triplets consist of three values created for a specific IMSI: a random number RAND, the corresponding response SRES and the corresponding session key K_c.

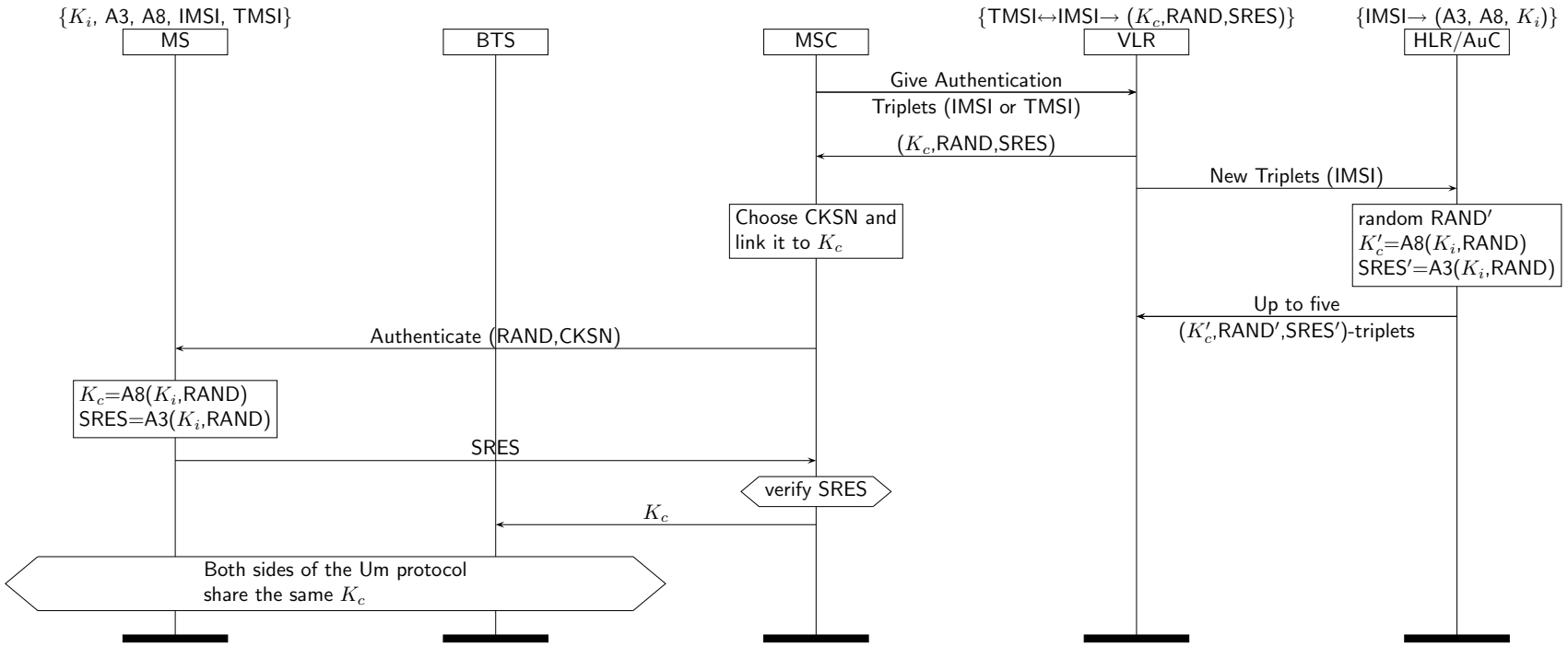

Figure 2.2: Global overview of successful authentication of an MS inside a GSM network. Upon request of the MSC the VLR supplies authentication triplets (K_c,RAND,SRES) – which it obtained from the AuC – with which the MSC authenticates the phone. Then the K_c is sent on to the BTS, which *can* now start to encrypt its communication with the phone.

These authentication triplets are created by the AuC, since this is the only instance that knows the K_i and A3 and A8 algorithms, belonging to the specific SIM card, and are stored at the VLR. If the VLR runs out of authentication triplets for the IMSI it will request up to five new triplets from the AuC, illustrated by the "New Triplets" command in Figure 2.2.

Figure 2.2 also uses a new value that was not yet discussed; the Ciphering Key Sequence Number (CKSN). The CKSN is chosen by the MSC and used as an identifier for the current K_c, once it receives an authentication triplet. If at some point later the communication between this MS and the network is to be encrypted, the network will refer to the session key by its CKSN. If the MS recognizes this CKSN it will use the accompanying session key. If the CKSN is not recognized the entire authentication needs to be repeated for a different authentication triplet.

About halfway in the diagram the actual authentication commences, represented by the "Authenticate" command transmitted to the MS accompanied by the challenge RAND and the CKSN. The MS computes the corresponding response, SRES, and session key, K_c, using the K_i, A3 and A8 known to it. The session key is stored alongside the CKSN and the response is tranmitted back to the MSC. The MSC verifies that the response is indeed correct, and if so it can send the session key on to the cell tower (BTS) to set up an encrypted connection.

Note that in this scheme only the SIM (as a part of the MS) and the AuC know the secret key K_i (and the algorithms A3 and A8). None of the other entities should be able to learn the K_i.

2.3 A3 & A8

The implementations of the A3 and A8 algorithms for every user exist only in two places; the SIM of the user and the providers' Authentication Centre (AuC). Both of these are controlled by the provider. So providers are free to choose the actual implementations of the A3 and A8 algorithm, as long as they follow the contracts of A3 and A8. For A3 this means that given two arguments, a 128 bit K_i and a 128 bit random (RAND) yields a 32 bit Signed Response (SRES). For A8 this means that given two arguments, a 128 bit K_i and a 128 bit random (RAND), result in a 64 bit session key (K_c). Both A3 and A8 should be implemented by cryptographic hash functions. Even though providers are free to choose their own implementation nearly all providers started out by using use the COMP128 algorithm, suggested by the ETSI for both A3 and A8 [6].

COMP128 was an example design by the ETSI given in a memorandum of understanding. It is a proprietary hash function that was kept confidential. In 1998 it was reverse engineered by Briceno, Goldberg, and Wagner [10], using a leaked document [11] and an actual GSM phone. Some improvements were introduced into a newer version of COMP128: COMP128v2, retrospectively renaming the original algorithm to COMP128v1. The second version is also kept secret, as are possible other A3/A8 algorithms. Currently the designs of the A3/A8 algorithms used in newer SIM cards is unknown.

2.3.1 COMP128v1

COMP128v1 performs both the A3 (response calculation) and the A8 (session key calculation) in a single algorithm. It is a cryptographic hash function that receives two 128 bit arguments

(the secret key K_i and the challenge RAND), and returns a 128 bit result. From this result the first 32 bits are used as the response (SRES). The session key (K_c) is formed by taking the last 54 bits and adding ten 0's to make up the 64 bits needed for the session key. It is unknown if this also happens in COMP128v1's successors.

COMP128v1 is a hash function with 40 rounds, where each round consists of a table look up followed by mixing. There are five different tables, one used for each consecutive round, which is repeated eight times. Source code of the entire COMP128v1 function can be found at [10].

Chapter 3

Encryption

This chapter explains the use of encryption on the GSM air interface. Encryption can be used in GSM to achieve some form of *call confidentiality*.

3.1 Encryption inside the GSM network

As we have seen in Chapter 2 the session key K_c by which communication can be encrypted is computed by the AuC and inside the SIM card. The AuC passes the key on to the MSC, from where it is eventually transmitted to the BTS. Similarly the SIM card passes the key on to the ME (the mobile phone hardware). So where authentication happens between SIM and network and is verified at the MSC, encryption is performed in the ME and the BTS.

Figure 3.1 shows the possibly encrypted links in a GSM network during a phone conversation. You can see that in an encrypted conversation, only the link between a phone and the cell tower (BTS) is encrypted. In a conversation between two mobile phones both of the BTS-Mobile phone links are encrypted under a different session key. So a speech packet from the first phone is encrypted under key K_{c1} (shared between the MS and the BTS) and transmitted to the nearest BTS. There the package is decrypted and send on into the GSM network. When it reaches the BTS currently serving the second phone, the speech packet is again encrypted, but this time under key K_{c2}, and transmitted to the second phone, where it is once again decrypted and finally finds it goal in the phone's speaker. For more information on all these three letter acronyms populating a GSM network see the Chapter **??**.

3.2 The encryption algorithms

Encryption in GSM is performed by one of the, currently three, A5-encryption algorithms.

Unlike the A3 and A8 algorithms, the A5 encryption is programmed into the phone hardware (ME) – A3 and A8 are programmed on the SIM – and in the cell towers (BTSs), and therefore there is only a choice between three pre-defined algorithms: A5/1, A5/2 and A5/3. These algorithms encrypt the payload of the communication, under the session key (K_c) and the current frame number. It is worth noticing that there is a fourth option, namely using no encryption. The mobile phone informs the BTS on which of the A5 encryption algorithms it supports. The BTS then decides whether to use encryption, and if so which algorithm to

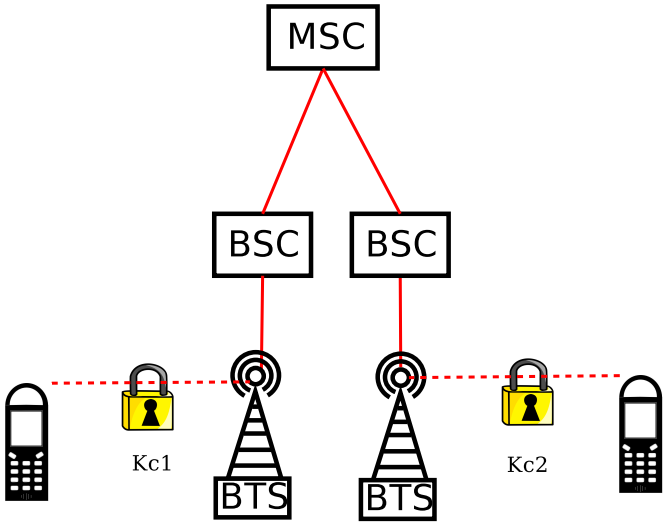

Figure 3.1: Possibly encrypted connections during a phone call. Note that only communication between the phones and the base stations is encrypted – whithin the GSM network the communication is unencrypted.

use, and sends this to the MS over a control channel.

A5/1 was the original encryption algorithm used in GSM. It was introduced in 1987, but at that time is was an export restricted encryption algorithm. So when GSM grew beyond Europe, a modified (and actually weakened) version was created: A5/2.

Originally the designs of A5/1 and A5/2 was kept secret. It was only disclosed to GSM manufacturers under NDA. However, in 1999 Marc Briceno reverse engineered the design of both A5/1 and A5/2 from a GSM phone [12]. Both algorithms are stream ciphers, generating keystream from the current frame number and the session key (K_c) which is XOR-ed with the plain text.

In 2002 an additional A5 algorithm was introduced: A5/3. Unlike with its predecessors, the design of A5/3 where immediately published [13]. It was based on the block-cipher KASUMI, which was already used in third generation networks, and which in turn was based on the block-cipher MISTY (KASUMI is the Japanese word for "mist"). A5/3 is currently considered unbroken and the best cryptographic alternative in GSM. A5/3 differs from its predecessors in yet another way; it uses a 128 bit session key, instead of 64 bits. Using 128 bits session keys is the standard in third generation mobile communication networks, but in GSM the session key provided by the A8 algorithm is defined as 64 bits. How these 64 bits lead to the 128 bit session key is currently unknown, but it seams unlikely that the session key in A5/3 will have more than 64 bits of entropy.

In January of 2010, Dunkelman, Keller and Shamir published a new attack on KASUMI reducing the time-complexity down to 2^{32}[14]; the previous best attack had a time-complexity of 2^{76}. This new attack is a so-called 'related key' attack and needs chosen plain text messages, making it impractical as an attack against GSM or the third generation networks. However, this theoretical attack is still worrying considering that the designers of KASUMI payed specific attention to related key attacks. Also this attack on KASUMI does not break MISTY

in any way, indicating that the changes made for KASUMI actually weakened the cipher significantly.

3.2.1 A5/1

Communication on the GSM air interface is send in bursts of a standard size. These bursts contain 114 bits of plain text. For each burst A5/1 generates 228 bits of keystream. Half of these are used to encrypt transmitted bursts and the other half are used to decrypt received bursts. A mobile phone uses the first 114 bits to encrypt its tranmission and the last 114 bits to decrypt the received signal. Cell towers do this just the other way around.

The encryption and decryption steps work by XOR-ing the 114 bits of keystream with the 114 bits of plaintext in a burst.

The internal design of A5/1 contains three Linear Feedback Shift Registers (LFSRs) of different size, named R1, R2 and R3, as is shown in Figure 3.2. These registers achieve irregular clocking through their *clock bits*. At the end of every step the three clock bits (bit 8 of R1 and bit 10 of R2 and R3) are compared to find the value of the majority of these three bits. Those registers with a clock bit that is equal to this majority will clock. So at each step two or all three of the registers will clock and each register will clock with a chance of $\frac{3}{4}$.

When a register clocks its *tap bits* (for R1 bits 13, 16, 17, and 18, for R2 bits 20 and 21 and for R3 bits 7, 20, 21 and 22) are XOR-ed and the resulting bit value is input at index 0 of the specific register. All bits inside the register move on to the next index. The highest number bits coming out the registers are XOR-ed together to form a keystream bit.

The internal state of the A5/1 cipher needs to first be instantiated with two variables; the session key (K_c) and the current frame number (FN). The session key is a private key that both MS and network can compute (see Chapter 2) and the frame number is a 22 bit, publicly known value that functions as a counter.

The A5/1 algorithm runs as follows:

1. Set all the registers to '0'
2. For $i = 0$ to 63:
   - clock all three registers
   - R1[0] $\leftarrow$ R1[0] $\oplus$ $K_c[i]$; R2[0] $\leftarrow$ R2[0] $\oplus$ $K_c[i]$; R3[0] $\leftarrow$ R3[0] $\oplus$ $K_c[i]$.
3. For $i = 0$ to 21:
   - clock all three registers
   - R1[0] $\leftarrow$ R1[0] $\oplus$ FN[i]; R2[0] $\leftarrow$ R2[0] $\oplus$ FN[i]; R3[0] $\leftarrow$ R3[0] $\oplus$ FN[i].
4. Run for 100 rounds using majority clocking. Discard the resulting output bits.
5. Run for 114 rounds using majority clocking. The resulting 114 output bits form the keystream used to decipher / encipher the next *downlink* package.

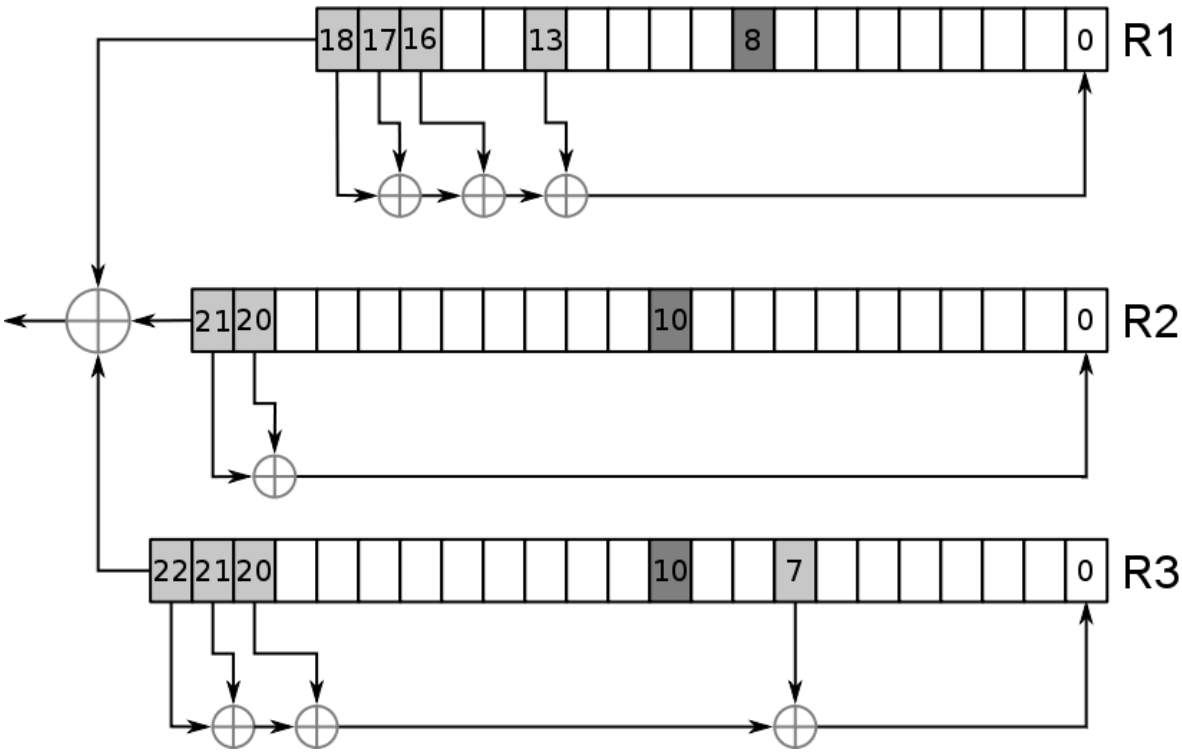

Figure 3.2: Diagram of the internal design of the A5/1 stream cipher.

6. Run for 114 rounds using majority clocking. The resulting 114 output bits form the keystream used to decipher / encipher the next *uplink* package.

7. Start again at step 1 with the same K_c and a new (current) FN.

Steps 1 to 4 show the initialization steps of the A5/1 algorithm. First the session key is clocked in, then the frame number follows. These initialization parameters are clocked in 'normally'. That is to say all three will clock simultaneously for every bit of the frame number and session key. After that the initialization phase is ended by clocking one hundred times using the majority clocking explained above.

The internal state is then ready to produce the keystream. In steps 5 and 6 the registers clock irregularly for 228 bits. This results in 114 bits of keystream used for encryption and 114 bits used for decryption. This handles the encryption of the next burst to transmit and the decryption of the first burst to receive. After that the entire process repeats itself for the next bursts in the next TDMA frame.

Bibliography

[1] John G. van Bosse and Fabrizio U. Devetak. *Signaling in Telecommunication Networks*, chapter 12. Wiley Series in Telecommunications and Signal Processing. Wiley-Interscience, 2 edition, 2006. ISBN: 0471662887.

[2] Joerg Eberspaecher, Hans-Joerg Voegel, and Christian Bettstetter. *GSM Switching, Services, and Protocols*. Wiley, 2 edition, 2001. ISBN: 047149903X.

[3] September 2009. `http://openbts.sourceforge.net/`.

[4] March 2009. `http://openbts.blogspot.com/`.

[5] September 2009. `http://bs11-abis.gnumonks.org/trac/wiki/OpenBSC`.

[6] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*, chapter 17. Wiley Computer Publishing, 2001. ISBN: 0471389226.

[7] European Telecommunications Standards Institute, France. *Digital cellular telecommunications system (Phase 2); International Mobile station Equipment Identities (IMEI)*, 2000. ETS 300 508 / GSM 02.16.

[8] International Telecommunication Union. *ITU-T Q.700 : Introduction to CCITT Signalling System No. 7*, 1994. (03/93).

[9] European Telecommunications Standards Institute, France. *Digital cellular telecommunications system (Phase 2+); Security related network functions*, 1998. ETS 300 929 / GSM 03.20.

[10] Marc Briceno, Ian Goldberg, and David Wagner. An implementation of the GSM A3A8 algorithm. (specifically, COMP128.), 1998. `http://www.scard.org/gsm/a3a8.txt`.

[11] Technical information GSM system security study. `http://cryptome.org/jya/gsm061088.htm`.

[12] Marc Briceno, Ian Goldberg, and David Wagner. A pedagogical implementation of the gsm a5/1 and a5/2 "voice privacy" encryption algorithms, 1999. `http://cryptome.org/gsm-a512.htm` (originally on `www.scard.org`).

[13] 2002. `http://cryptome.org/a53-gea3/a53-gea3.htm`.

[14] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time attack on the a5/3 cryptosystem used in third generation GSM telephony. 2010. `http://eprint.iacr.org/`.